C-Prot

Cognitive Protection

FOR HOME

FOR BUSINESS

FOR IoT

FOR MOBILE

C-Prot

www.c-prot.com

ABOUT US

C-Prot; develops unique cyber security products that solve cyber security problems of users with innovative methods, address the global market that can be used on different platforms, and prioritise user experience. The cyber security products it develops are used in the protection of critical infrastructures such as defence industry, telecommunications, energy, banking, health, transportation and finance.

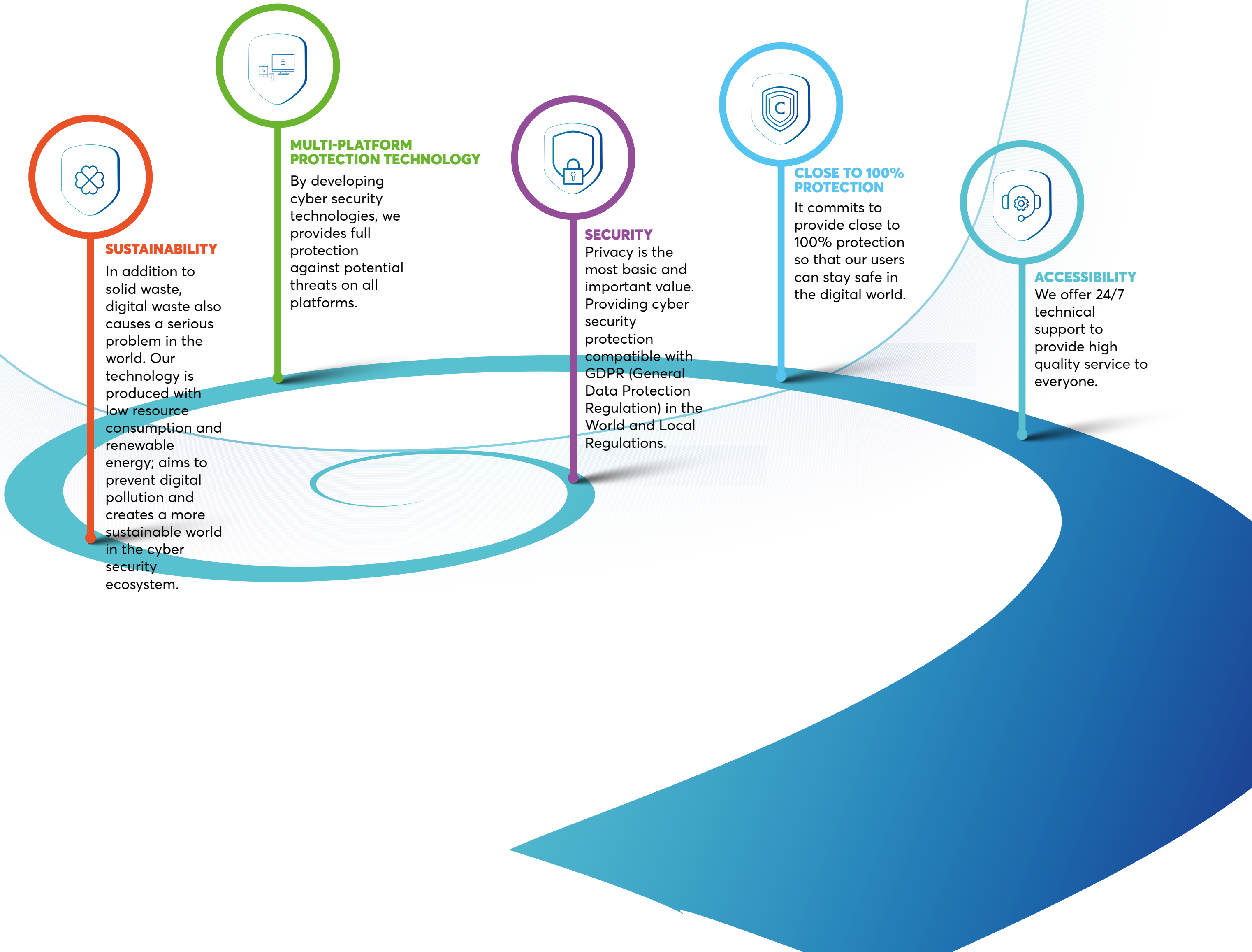
C-Prot has **OPSWAT, STARCHECK, SKD AWARDS, VB100** awards with the highest criteria that very few companies in the world have.

C-Prot is a member of the **"European Expert Group for IT-Security", the "Anti-Malware Testing Standards Organization"** and the **"Association of Asian Antivirus Researchers"**.

C-Prot will continue to keep you safe in the digital world with a wide range of high-tech cybersecurity products, from smart televisions to mobile devices, while maintaining its commitment to providing its customers with the best endpoint protection products.

BRAND VALUES

C-Prot produces cyber security products that work on all platforms with its own developed technologies which respect brand values.



SUSTAINABILITY

In addition to solid waste, digital waste also causes a serious problem in the world. Our technology is produced with low resource consumption and renewable energy; aims to prevent digital pollution and creates a more sustainable world in the cyber security ecosystem.

MULTI-PLATFORM PROTECTION TECHNOLOGY

By developing cyber security technologies, we provides full protection against potential threats on all platforms.

SECURITY

Privacy is the most basic and important value. Providing cyber security protection compatible with GDPR (General Data Protection Regulation) in the World and Local Regulations.

CLOSE TO 100% PROTECTION

It commits to provide close to 100% protection so that our users can stay safe in the digital world.

ACCESSIBILITY

We offer 24/7 technical support to provide high quality service to everyone.

AWARDS AND MEMBERSHIPS

OPSWAT PLATINUM

C-Prot has the highest criteria **OPSWAT Platinum** certificate that only a few companies in the world have.

STARCHECK

Functionality testing, performance verification and information security product As a result of the extensive tests carried out in 2022 by SKD Labs, an ISO / IEC 17025 accredited laboratory specialized in certification and certification of its products and services, and one of the 8 test centers in the world, the certificates of which are recognized by Microsoft, 99.99% malware detection, 100% Ransomware detection and 0% false positive success. It has been awarded the **"STARCHECK"** certificates for the 3rd time in a row with its corporate and individual products.

SKD AWARDS

C-Prot has won the individual awards in the **"SKD AWARDS"** awards, which is considered as the "Oscar of Cyber Security Products" by the industry and is considered as one of the important indicators in measuring the level of cyber security products, organized by the world-renowned independent testing and certification laboratory SKD Labs every year since 2013 and **"SKD AWARDS 2022 PRODUCT EXCELLENCE"** in corporate endpoint protection categories.

VB100

Virus Bulletin is a UK-based testing and certification Center with a great reputation for providing users with independent intelligence on the latest developments in the global threat lands cape since 1989. After being tested with nearly 50 different global security solutions in the unique independent comparative test series published by **"Virus Bulletin"** in May 2023, it was awarded the **"VB100"** award for the 12th time in a row with its individual and corporate products.

AWARDS AND MEMBERSHIPS

Deloitte.
50 Technology Fast 50 2020 Turkey
C-Prot
Deloitte Technology Fast 50 Turkey 2020 Runner Ups List Award

DELOITTE FAST 50

Within the scope of the Deloitte Technology Fast 50 program, which has been implemented in Turkiye since 2006, the fastest growing 50 technology companies in Turkiye are determined every year. C-Prot was awarded the **"Runner Ups"** award by entering the list of companies that produce its own technology, use advanced technology in problem solving and make serious R&D investments in technology, organized by Deloitte Turkiye, with a growth of 946%.

AMTSO

C-Prot has been accepted as a member of the worldwide **"Anti-Malware Testing Standards Organization".** AMTSO is an international non-profit organisation founded in 2008 to address a perceived need for improvement in the quality, relevance and objectivity of anti-malware testing methodologies. As of 2022, it includes 56 technology giant companies worldwide. As a member, C-Prot plays an active role in setting international test standards.

AVAR

C-Prot has been accepted as a member of AVAR **(Association of Anti Virus Asia Researchers)**, to which companies with global achievements can apply. AVAR focuses on the Asia Pacific region and works in collaboration with leading experts from 18 countries including Australia, China, Hong Kong, India, Israel, Japan, Japan, Korea, Philippines, Singapore, Taiwan, Turkiye, the United Kingdom and the United States.

EICAR

C-Prot has been accepted as a member of the **European Expert Group for IT-Security,** which is based in Europe and operates globally. EICAR was founded in 1991 and provides an independent and impartial platform for IT-Security experts in the field of science, research, development, implementation and management.

PRODUCTS

C-Prot; It is a global cyber security company. On individual and corporate platforms; It produces Android, Windows, Linux, MacOS, iOS, HarmonyOS and hardware-based cyber security products.

INDIVIDUAL PRODUCTS

- C-Prot Antivirus
- C-Prot Internet Security
- C-Prot Mobile Antivirus Security
- C-Prot AppLocker
- C-Prot Parental Control
- C-Prot Smart TV Security
- C-Prot Web Protection
- C-Prot Mobile VPN
- C-Prot QR Scanner

ENTERPRISE PRODUCTS

- C-Prot Endpoint Antivirus
- C-Prot Endpoint Security
- C-Prot Remote Administrator
- C-Prot Internet Security
- C-Prot Endpoint Smart TV Security
- C-Prot Cyber Security Kiosk
- C-Prot Embedded AppDefense
- C-Prot Device Fingerprint
- C-Prot Fraud Prevention
- C-Prot Threat Intelligence Portal

C-Prot Internet Security

Advanced protection against all threats with a single application.

Top Features

Real Time Protection
It detects threats in real time and blocks them before your device is damaged.

Online Payment Protection
It prevents hackers from intercepting your credit card details and financial data when conducting an online transaction on your computer.

Internet Protection
Prevents access to harmful websites. Automatically scans files downloaded from the Internet.

Ransomware Protection
It detects potentially harmful changes made to your sensitive data by malware and neutralises malware that encrypts your data.

Sectors Used

For Home:
For the safety of your children, the enjoyment of your gaming sessions and the security of your online banking transactions, you can fully protect your digital life with C-Prot.

E-commerce:
Companies and online stores can use it to secure customer information and payment details.

Finance:
The financial services industry, such as banks, financial institutions and investment firms, is used to protect customer accounts and financial data.

For Business:
Small businesses can use it to protect their business computers and networks from viruses, spyware and other online threats.

Healthcare:
Provides security against cyber threats in the digital world to protect patients' medical records and personal health information.

Telecommunication:
Telecommunication companies and internet service providers ensure the security of their employees in the digital world.

INTERNET SECURITY

Our comprehensive security plan provides enhanced protection against viruses, online threats and other threats.

Highlights

★ ★ ★ ★ ★

Anti-Malware

Protects your computer against viruses, spyware and other malware.

Automatic Update

During your licence term, it automatically updates against the latest threats.

C-Prot Boost Technology

This innovative technology helps C-Prot automatically configure scanning technology to efficiently utilise hardware and software resources and improve device performance.

Low Resource Consumption

It uses your system resources efficiently and protects your computer without slowing it down.

E-Mail Protection

Keeps unwanted or malicious e-mails out of your inbox, automatically scans attachments.

C-Prot Security Network

It provides high-level protection to your device with cloud-based protection technology on your devices.

Social Network Protection

Take precautions against risks that may come from social media platforms such as Facebook, X, Instagram.

Heuristic Protection

Behavioural scanning detects suspicious or threatening behaviour of malware and provides multi-layered protection for your device.

Secure Download

Automatically scans files downloaded from the Internet.

Self-Defense

The C-Prot self-defence feature provides a defence mechanism against malware or other malicious activity disabling C-Prot.

Phishing and Fraud Protection

It provides a high level of protection against malicious websites that want to capture your sensitive data such as your username, password, banking or credit card information.

Botnet Protection

Protects your device from being used maliciously as part of an infected computer network or as a "botnet".

Spyware Detection

It protects against malware that collects your device's information without authorisation.

Crypto Mining Protection

By effectively managing your computer's resources, it prevents crypto mining activities and provides a safe and efficient use. Thus, it makes you safer against cryptocurrency fraud.

Threat Log

It gives a summary of detected threats and more.

C-Prot Smart Tv Security

Advanced protection against all threats for Smart Televisions.

Top Features

Anti-Malware
Detection of malicious software present on your device is performed.

Scheduled Scan
You can start scanning your device for malware detection by specifying any day or time.

USB Protection
Your Smart Tv's protected against malware that may come to your device via USB storage devices.

Firewall
It monitors the internet traffic and network movements of the installed applications on the device.

Sectors Used

For Home:
Secures Smart TVs at home when shopping online, watching films and TV series or using social media.

Education:
Can be used to protect the security of Smart TVs for schools and educational institutions.

Hospitality:
It can be used to provide a secure digital experience for guests using Smart TVs in hotel rooms.

Healthcare:
Healthcare organisations can be used to secure medical information on Smart TVs used in waiting rooms or patient rooms.

Transportation:
It can be used to secure Smart TVs at transport hubs such as airports, railway stations and bus terminals.

Entertainment:
It can be used to secure Smart TVs used in entertainment venues in the digital world.

SMART TV SECURITY

C-Prot Smart TV Security is a powerful and award-winning antivirus security application designed specifically for the security of Smart TVs running on the Android TV operating system, prioritising high performance and low resource consumption. With real-time protection technology, it protects you against cyber threats by automatically detecting malware, ransomware, phishing attempts, spyware and other malicious software.

Highlights

★ ★ ★ ★ ★

Heuristic Protection

Against new and unidentified malware provides protection.

Smart Scanning

Protects your computer with a single, all-in-one scan.

On-Demand Scanning

With quick scan, full scan and custom scan options, you can activate it at any time to scan applications and files on your device for malware.

Secure Download

Automatic scanning of files downloaded from the Internet.

Quarantine

When malware is detected, you can isolate the malware by deletion or quarantine, and you can restore your files that you think are safe.

Low Resource Consumption

It uses your system resources efficiently and protects your device without slowing it down.

Automatic Update

During your licence term, it automatically updates against the latest threats.

Automatic Scanning

When you install a new application, it is automatically scanned by C-Prot Smart TV Security before you run it.

Advanced Settings

Using the advanced settings options, you can edit the protection options and enable Update and on-demand scheduled scans.

Get Started Easily

Open the Google Play Store. Find C-Prot Smart TV Security, download the App. Enjoy the free version or upgrade to the premium version to use additional features.

Provide top-level security for your Smart TV.

C-Prot Web Protection

Stay safe away from online scams, malicious websites, advertising and analytics trackers that track you online.

Top Features

Multiple Browser Support
It currently supports Chromium-based browsers (Google Chrome, Yandex, Opera, Edge, etc.).

Link Analysis
Enables internet addresses to be marked as safe or not secure.

Advanced Ad Blocking
You can block all of them, including all ad trackers, pop-ups and adverts.

Anti-Phishing
Protects you against phishing attacks on malicious websites.

Sectors Used

For Home:
For the safety of your children, the enjoyment of yourvgaming sessions and the security of your online bankingvtransactions, you can fully protect your digital life with C-Prot.

E-commerce:
Companies and online stores can use it to secure customer information and payment details.

Healthcare:
Provides security against cyber threats in the digital world to protect patients' medical records and personal health information.

For Business:
Small businesses can use it to protect their business computers and networks from viruses, spyware and other online threats.

Finance:
The financial services industry, such as banks, financial institutionsm and investment firms, is used to protect customer accounts and financial data.

Telecommunication:
Telecommunication companies and internet service providers ensure the security of their employees in the digital world.

WEB PROTECTION

With C-Prot Web Protection, stay safe away from online fraud, malicious websites, advertisements and analytics trackers that track you online. It provides protection by performing phishing attacks and malware analysis on the pages you visit with transactions made on the cloud.

Multiple Browser Support ✓
For now, it can only be used in Chromium-based browsers (Google Chrome, Yandex Browser, Opera, Edge, etc.).

Low Resource Consumption ✓
With its ad-blocking feature, it reduces CPU, memory and network usage, ensuring efficient use of your device and network traffic.

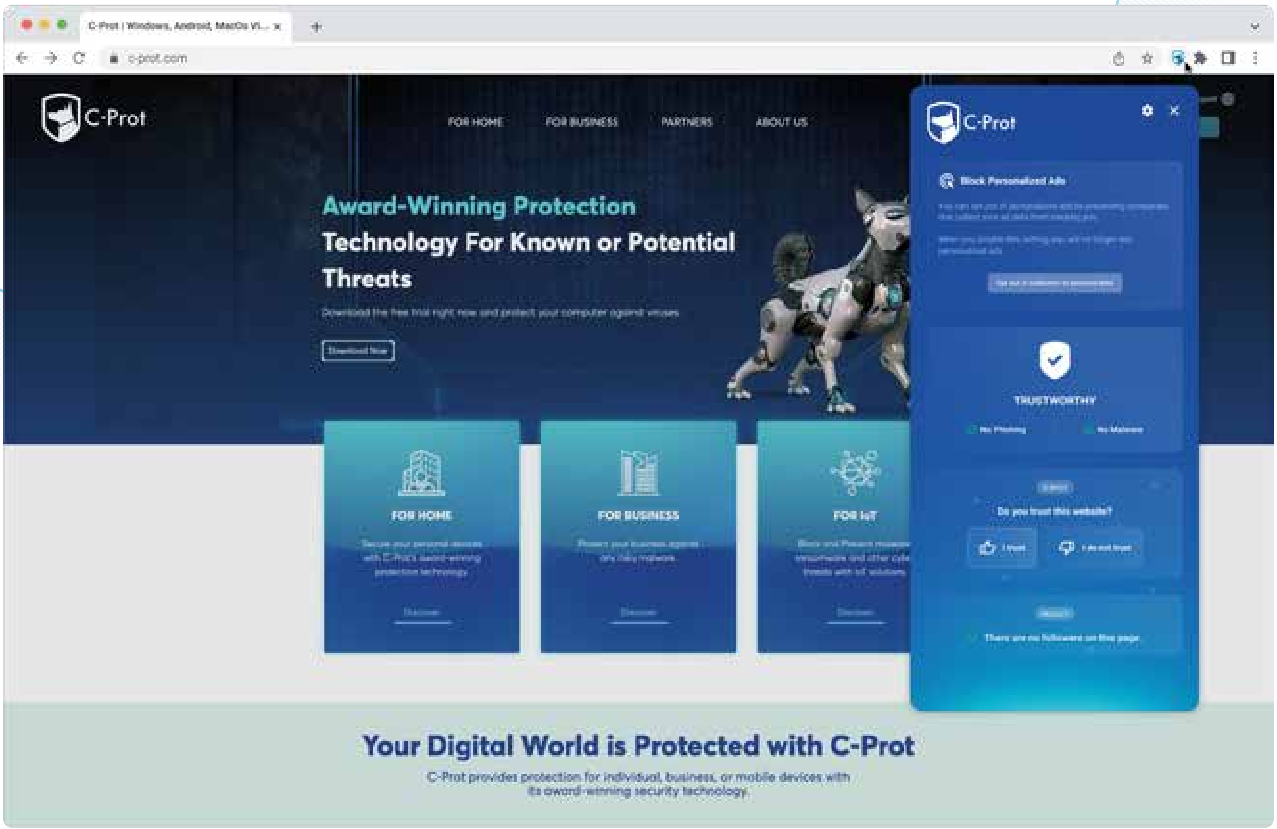
Advanced Ad Blocking ✓
C-Prot Web Protection detects ad trackers on the websites you visit and shows you which sites are tracking you. This protects your privacy by preventing your online activities from being tracked.

Link Analysis ✓
C-Prot Web Protection analyzes the reliability of the websites you want to visit and detects potentially harmful or unsafe links. Thus, it allows you to have a safe online experience.

High performance ✓
It speeds up page loading and saves bandwidth.

Anti-Phishing ✓
C-Prot Web Protection provides protection against phishing attacks. It detects harmful websites and potential phishing attempts, protecting and keeping your personal data safe.

Turning Off Ad Permissions ✓
C-Prot Web Protection provides an option to turn off ad permissions. In this way, it protects your privacy by preventing ads from interacting with you and prevents unwanted ads from contacting you.



Award-Winning Protection Technology For Known or Potential Threats

Download the free trial right now and protect your computer against viruses

FOR HOME

FOR BUSINESS

FOR IoT

Do you trust this website?

There are no followers on this page

Your Digital World is Protected with C-Prot

C-Prot provides protection for individual, business, or mobile devices with its award-winning security technology.

C-Prot Endpoint Security

Advanced protection that can be managed on-premises or in the cloud with a single application against all threats.

Top Features

Anti-Malware
Protects computers, servers and mobile devices in your organization against risks from viruses, trojans, worms and ransomware.

External Media Management:
You can limit or control the use of undefined external devices (USB drives, CD/DVD drives, external hard drives, etc.).

Central Management Console
Manage all your endpoints from anywhere with C-Prot Remote Administrator, available as cloud-based or on-prem.

Policy Management:
You can configure multiple policies with different values. An application may run under different settings for different administrative groups.

Sectors Used

Finance:
Develops endpoint protection solutions for organisations providing financial services, including banks, financial institutions and insurance companies.

Healthcare:
Provides security against cyber threats in the digital world to protect patients' medical records and personal health information.

Critical Infrastructure:
Protects against cyber threats in the digital world to prevent power outages in power generation, transmission, utilities and critical infrastructure.

Manufacturing:
Provides security in the digital world to prevent interruptions in production processes and defend against industrial espionage.

Government:
Provides protection against cyber threats that government and public sector organisations may face in the digital world.

Education:
The C-Prot Endpoint Security product has been developed to protect the information of educational institutions, students and staff against cyber attacks.

Retail:
Provides protection in the digital world to safeguard customer data and payment information.

Telecommunications:
Telecommunications companies and internet service providers can use this to protect their computers at endpoints.

ENDPOINT SECURITY

C-Prot Endpoint Security is designed to keep you safe in the digital world, while enabling you to use your devices with high performance. C-Prot Endpoint Security blocks the risks posed by all kinds of viruses, spyware, trojans, worms, adware and other threats. In addition, while you do your daily work, it provides superior protection without tiring your device and reducing its performance. Thanks to internet and e-mail protection, it continues to protect you in the internet environment. With heuristic protection technology feature It provides full protection to your device. Using C-Prot Endpoint Security together with C-Prot Remote Administrator in a corporate environment, you can easily manage multiple client workstations, enforce your policies and policies, and configure them remotely from any network computer.

Highlights

★ ★ ★ ★ ★

Advanced Machine Learning Technology

It offers superior protection technology by utilizing the latest machine learning developed against new and unidentified malware.

Distributed Update Structure

Create multiple distribution points to avoid putting extra load on the servers while updating the application and signature database.

Internet-Using Applications

Instantly see the internet traffic of the applications and block the application you want.

Phishing and Fraud Protection

It provides high-level protection against malicious websites that want to capture your sensitive data such as your username, password, banking or credit card information.

Online Payment Protection

It prevents hacking of your credit card information and financial data while conducting an online transaction on devices in your institution.

Botnet Protection

It protects devices in your organization from being misused as part of an infected computer network or as a "botnet".

Anti-Theft

It helps you track and locate your devices in case of loss or theft.

Self-Defense

C-Prot's self-defense feature provides a defense mechanism against malware or other harmful activities from disabling C-Prot.

E-mail Protection

Keeps and blocks spam or malicious e-mails out of your inbox. Thus, it prevents your employees from clicking on harmful e-mails and ensures protection against phishing attacks.

Patch Management

Strengthen security with automatic patch management; possible in software, operating systems, and applications. reduce the risk of security vulnerabilities.

Spyware Detection

It provides protection against malicious software that collects the information of devices in your organization without permission.

Low Resource Consumption

It uses system resources efficiently and protects your computer without slowing down.

Firewall

C-Prot Endpoint Security offers an integrated firewall. This firewall monitors network traffic and blocks harmful or unwanted connections. It also ensures the security of data entering and leaving your organization's network.

Mobile Threat Protection

It provides comprehensive protection by detecting spyware, viruses and other malicious applications on mobile devices in your organization.

C-Prot Threat Intelligence Portal

Integrate continuously updated threat intelligence feeds into security controls such as SIEM (Security Information and Event Management) systems.

Top Features

Threat Intelligence and Analysis
It provides constantly updated threat intelligence to track malware samples, the latest threats and vulnerabilities.

File and Hash Analysis
Detect all threats using our global cloud reputation system, including dynamic, static and behavioural analysis.

API Access
Provides APIs that support your security team or automation tools to access threat information and create automated responses.

Malware Analysis
Access detailed information on specific malware indicators, as well as the tools, tactics, and attack types used by cyber attackers.

Sectors Used

Finance:
Protecting banks, financial institutions and insurance companies against cyber threats can use the threat intelligence service.

Healthcare:
Hospitals and healthcare organisations can use threat intelligence services to protect against threats to patient records and sensitive health data.

Critical Infrastructure:
Energy companies, infrastructure providers can use threat intelligence services to protect critical infrastructure and protect against cyber threats.

Manufacturing:
Threat intelligence service can be used to protect against cyber attacks against industrial production facilities.

Government:
Governments, ministries of defence, intelligence agencies and others can use the threat intelligence service to protect their sensitive data.

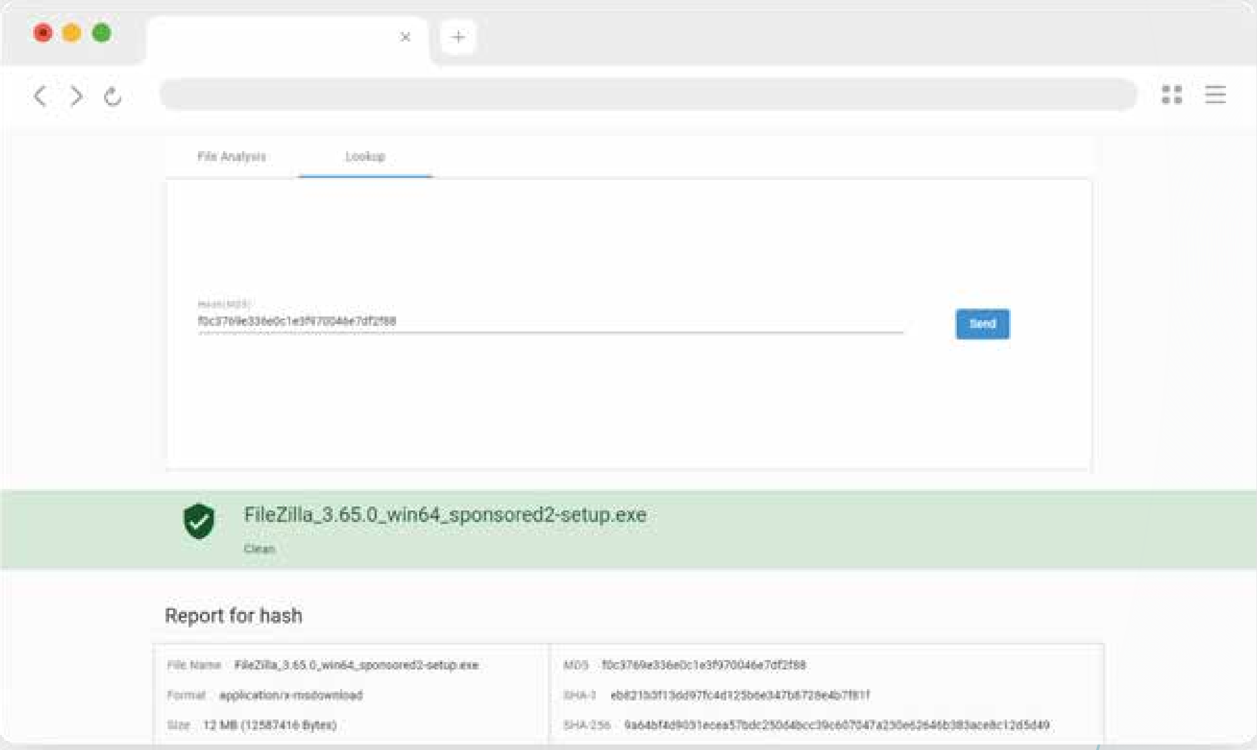
Education:
Universities and educational institutions can use the threat intelligence service to protect student data and against cyber attacks.

Retail:
Companies in the retail sector can use a threat intelligence service to protect customer payments and personal information against cyber threats.

Telecommunications:
Telecommunications companies and internet service providers can use threat intelligence to protect their customers communication networks.

THREAT INTELLIGENCE PORTAL

C-Prot Threat Intelligence Portal is a powerful web service for providing access to information about cyber threats. C-Prot Threat Intelligence Portal offers the possibility to check different types of suspicious threat indicators such as file, file signature, IP address or web address. In this way, institutions are informed about potential threats and can take necessary precautions. Understand threat trends and anticipate specific attacks with complete knowledge of your threat environment. Strengthen your defense mechanism with detailed information on offensive behavior and infrastructure.



Hash (MD5)
f0c3769e336e0c1e3f970046e7df2f88

FileZilla_3.65.0_win64_sponsored2-setup.exe

Clean

Report for hash

File Name FileZilla_3.65.0_win64_sponsored2-setup.exe	MD5 f0c3769e336e0c1e3f970046e7df2f88
Format application/x-msdownload	SHA-1 eb821b3f136d97fc4d125b6e347b8728e4b7f81f
Size 12 MB (12587416 Bytes)	SHA-256 9a64bf4d9031ecea57bdc250d4bcc39c607047a230e62646b383ace8c12d5d49

Global Threat Intelligence It provides comprehensive threat intelligence. Global Threat Intelligence; includes attack samples, malware samples, attack analytics, and other threat information.	✓
Malware Analysis Access detailed information on specific malware indicators, as well as the tools, tactics, and attack types used by cyber attackers.	✓
File and Hash Analysis Detect advanced threats using our advanced detection technologies, including dynamic, static, and behavioral analysis, and our global cloud reputation system.	✓
Strategic and Operational Threat Intelligence Understand threat trends and anticipate specific attacks with complete knowledge of your threat environment. Strengthen your defense mechanism with detailed information on offensive behavior and infrastructure.	✓

C-Prot Device Fingerprint

Identify your web and mobile visitors with the most accurate device identification platform.

Top Features

Unique Digital Fingerprint
It generates a unique digital fingerprint identifier for users by analyzing browser and device features with special algorithms.

Easy Integration for Developers
Easily add C-Prot DFP SDK to your applications get started quickly by integrating.

Country, City, Time Zone Change Detection
It detects when users appear in a different location than the country, city and time zone specified in their previous entries.

Fast Travel Detection
It detects whether the location change has been made within the period specified in the manage-ment panel.

Sectors Used

Finance:
Banks and financial institutions can improve account security by recognising users' devices. They can also use it to strengthen fraud detection and authentication processes.

Healthcare:
Provides security and access control for healthcare services. Strengthens authentication and authorisation processes. Protects the confidentiality of medical data.

E-Commerce:
Distinctly recognise potential fraudsters visiting your trading platform by detecting them with an exceptional accuracy rate of close to 100%.

Advertising:
Used for target audience identification and segmentation. It is used to show the right adverts to the right users. Prevents advert fraud.

Cryptocurrency:
With a state-of-the-art scanner fingerprint API with close to 100% accuracy, you can detect and block crypto fraudsters who want to steal account data and transfer money to their own wallets.

Online Gaming:
Allows you to fight against common gaming and gambling fraud techniques, including automatic credential stuffing, fraudulent strategies and various other illegal activities.

DEVICE FINGERPRINT

C-Prot Device Fingerprint is a solution developed to securely identify users and analyze web traffic on websites. This solution aims to provide high-level security and improve user experience by uniquely identifying users.

Highlights

★★★★★

Device ID Spoofing Detection

Application information may change on rooted devices. This information is determined whether it is changed or original.

Bot Detection

It determines whether a bot like Selenium or a real human is using the browser.

Central Management Console

Available as cloud-based or On-prem Manage all your endpoints with C-Prot Remote Administrator ıt allows you to manage from anywhere.

Malicious User Detection

Incompatible time zones, use of incognito mode and malicious users with features such as proxy and pinpoints it precisely.

VPN and Proxy Usage Detection

It analyses the user's IP address to determine whether this address belongs to a VPN or proxy server.

Remote Connection Detection

C-Prot Device Fingerprint detects users who access via remote desktop connection programmes such as AnyDesk, TeamViewer.

Incognito Tab Usage Detection

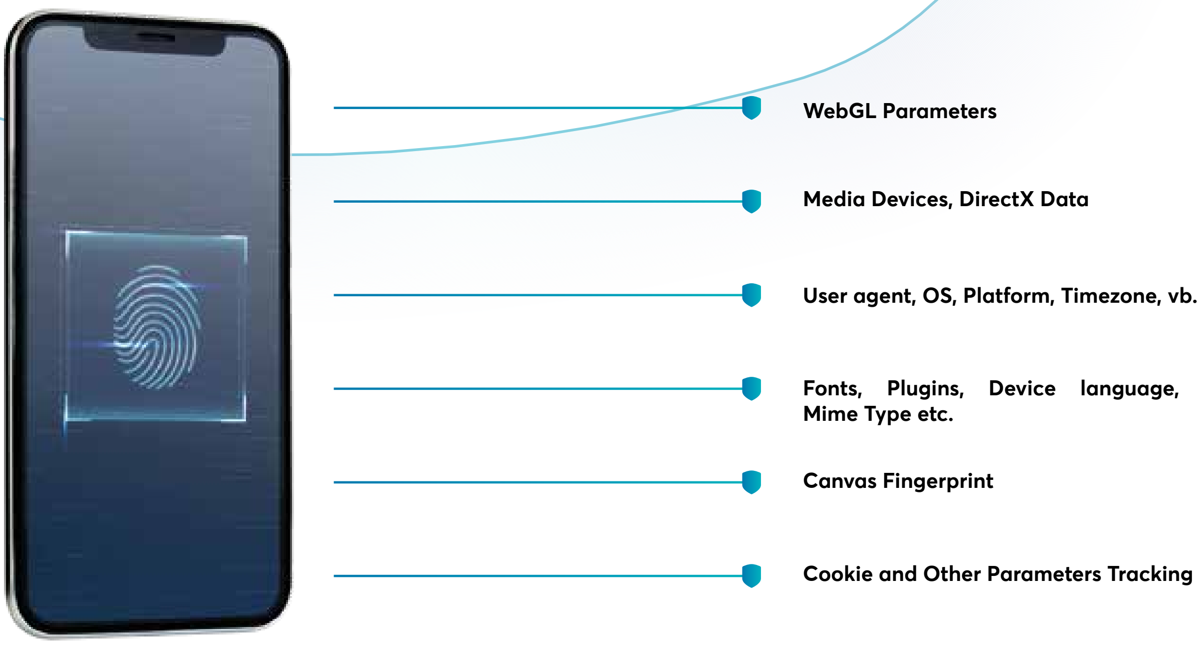
Detects users who access websites in private browsing mode.

Automation Usage Detection

It detects the requests made by web automation tools targeting Internet addresses.

Multiple Account Detection on Device

It detects multiple logged in users on the same browser.



WebGL Parameters

Media Devices, DirectX Data

User agent, OS, Platform, Timezone, vb.

Fonts, Plugins, Device language, Mime Type etc.

Canvas Fingerprint

Cookie and Other Parameters Tracking

C-Prot Fraud Prevention

Prevent fraud and provide a seamless digital experience for your customers.

Top Features

Anti-Fraud and Security
It can detect and prevent fraud attempts using fingerprint data from users' devices.

Remote Connection Detection
It is determined whether the device is used by remote desktop applications or by the user himself.

Behaviour Analysis
It uses a system behaviour analysis that analyses user behaviour and analyses it to identify abnormal or potentially fraudulent activities.

Root/JailBreak Detection
It provides an additional layer of defence against fraudsters by detecting operating system changes made to the user's device.

Sectors Used

Finance:
Enhances financial security during online banking, detectsphishing attempts and prevents malware.

E-Commerce:
Blocks fraudulent websites, secures customer payments, and protects against phishing attempts.

Insurance:
Prevents fraud, detects fraudulent claims and protects customer data.

Healthcare:
Secures health records, detects phishing attempts and protects against prescription fraud.

Transportation:
Protects travel bookings, secures customer card informationand prevents phishing attempts.

Telecommunications:
Detects phishing attempts, prevents account fraud, and secures subscriber information.

FRAUD PREVENTION

Features for the Mobile Channel

Mobile App Protection: C-Prot Fraud Prevention detects and blocks fraudulent attempts in mobile applications, providing robust defense against malicious apps and fake app stores.

Device Recognition and Identity Verification: It offers identity verification using unique features of mobile devices, thereby detecting fraudulent attempts originating from counterfeit devices.

Push Notification and SMS Security: Security is ensured for push notifications and SMS messages received on mobile devices to prevent fraudulent attempts.

Mobile Wallet Security: It safeguards mobile payment and wallet applications, ensuring the security of financial transactions.

Features for the Web Channel

Advanced Browser Protection: C-Prot Fraud Prevention detects malicious software and fraudulent activities operating within web browsers, enabling users to browse the internet securely.

Phishing Prevention: Phishing Prevention: It identifies and blocks fake websites and phishing attempts, protecting users from such cyber threats.

SSL Certificate Monitoring: It tracks SSL certificates crucial for secure communication and detects fraudulent attempts.

E-commerce Security: It safeguards e-commerce websites, especially during online shopping, and secures customer payments.

Online Banking Security: It secures internet banking transactions and protects users' financial information.

Key Benefit

Cyber Fraud Protection: C-Prot Fraud Prevention safeguards users against cyber fraud attempts, offering a robust defense against various types of cyber threats, including phishing, malware, fake websites, and many others.

Financial Security: It ensures the protection of users' financial information and payments by ensuring the security of mobile wallets and online banking transactions.

Advanced Identity Verification: By providing identity verification for both mobile and web channels, it detects fraudulent attempts and enhances user credibility.

Real-time Monitoring: C-Prot Fraud Prevention employs real-time monitoring to instantly detect fraud attempts and provide users with swift alerts.

Customizable Policy Controls: It offers customizable policy controls that can align with the specific needs of each business, allowing them to tailor fraud protection according to their requirements.

Mobile and Web Compatibility: With optimized features for both mobile and web channels, it ensures users' safety on both platforms.

Education and Support: C-Prot provides customers with cybersecurity education and continuous support, fostering awareness and enhancing security for businesses and individuals.

Ease of Integration: Depending on the needs, various integration methods such as cloud or on-prem are also offered.

FRAUD PREVENTION

C-Prot Fraud Prevention is a comprehensive solution that helps organisations detect and prevent fraud attempts such as financial fraud, phishing and money laundering through mobile and web channels. Depending on the needs, various integration methods such as cloud or on-prem are also offered.

Highlights

★ ★ ★ ★ ★

Behavioural Biometrics

It offers a technology that analyses customers' interaction with their devices such as mouse movements, clicks, taps, scrolling speed and more to determine whether a device is being used by a legitimate user. It evaluates the user's real-time interactions and creates a unique user profile.

SMIPhising

It detects if there is information on the phone for SMS fraud.

Sim Card Change Detection

It determines whether the user has a sim card in the device and whether the sim card has been changed.

Fast Travel Detection

The panel detects whether a position change has been made within the specified time.

Device ID Spoofing Detection

Application information may change on rooted devices. This information is determined whether it is changed or original.

Bot Detection

It determines whether a bot like Selenium or a real human is using the browser.

User Agent Spoofing Detection

The information of the browser used by the user may change. The information of the browser is detected whether it is original information or fake information.

VPN / Proxy Detection

It is determined that the user is connected via VPN.

Tor Browser Detection

It is determined whether the user is using Tor Browser or not.

Country, City, Time Zone Change Detection

It detects when users appear in a different location than the country, city and time zone specified in their previous entries.

Multiple Account Detection on the Device

When detecting a registered phone logging into the user's device, it also detects people using guest mode.

C-Prot Embedded AppDefense

Provide lightweight, embedded SDK protection for your applications against all threats.

Top Features

Anti-Malware
Detection of malicious software present on your device is performed.

Emulator Detection
It is determined whether the application works on a real device.

Device Fingerprinting
Creates a unique digital fingerprint identifier for your devices.

Suspicious Call Detection
Calls from unknown, suspicious numbers or fraud attempts are detected.

Sectors Used

Finance:
It enables banks, financial institutions and similar companies to securely protect their customers' financial information.

Retail:
Retail networks, especially those with in-app shopping capabilities, ensure that their customers' payment information is processed securely.

Transportation:
Companies offering vehicle services, especially rental and sharing services, Taxi and similar services ensure the protection of their customers' personal information.

Hospitality:
It ensures that the personal and financial information of its customers is processed securely.

Government:
It can be used to protect sensitive data contained in mobile applications developed by governments, ministries of defence and public institutions.

Manufacturing:
Ensures the security of mobile applications used in the manufacturing sector in the digital world.

EMBEDDED APPDEFENSE

Risks and Solutions on Mobile Applications

Detect Rooted Android Devices

Research around the world shows that 36 out of every thousand Android devices are rooted. Rooted Android devices have become a tool that cyber attackers can use to change the behavior of applications or steal sensitive data. C-Prot Embedded AppDefense offers automatic rooted device detection to ensure your app only works in secure Android environments.

What are the Risks that Rooted Device Users May Encounter?

Loss of Control on Devices: On rooted devices, hackers can modify your app, run scripts that steal data, and even compromise non-shared spaces like your app sandbox.

Malware Attacks: Rooted devices make it easy for hackers to carry out malware attacks. It also simplifies updating and automating processes. These devices often allow sensitive personal data to be stolen from the device.

Detect Jailbroken iOS Devices

Apps running on a jailbroken iOS device have more privileges than Apple intended. To protect against malware and other risks posed by jailbroken devices, it's essential to secure your apps with solutions that detect and automatically respond to vulnerable conditions. After the integration of C-Prot EAD SDK product into your application, you can easily detect jailbroken devices. You can prevent your app from running on jailbroken device.

What are the Risks that Jailbroken Device Users May Encounter?

Unprotected Devices: Jailbroken devices allow attackers to manipulate users (e.g. in-app purchases) and bypass security checks.

Data Privacy Violations: Leaving your app vulnerable to jailbroken devices can allow cybercriminals to easily steal your users' personal data, resulting in costly fines, reduced stocks and loss of customer trust.

Overlayed Device Detection

A Screen Overlay Attack is a mobile app cyberthreat in which a malicious app shows an overlay over a legitimate e-commerce or bank app on a device. This deceptive technique tricks users into unknowingly granting sensitive permissions or interacting with rogue interfaces to lead to potential data theft, unauthorized access, or fraudulent activity. By presenting an overlay that mimics the appearance of a trusted app or system prompt, attackers can trick users into providing sensitive information such as login credentials or financial details.

With its Overlay detection feature, C-Prot Embedded AppDefense detects whether users have an overlay on their screen while using an application. Overlay attacks are used to capture users' personal and financial data. C-Prot Embedded AppDefense detects such attacks and provides a secure user experience.

Key Benefit

Multi-Platform Compatible: C-Prot EAD enhances existing mobile applications and enables businesses to secure mobile transactions on devices running Android or iOS operating systems.

Protect Your Devices: C-Prot EAD is designed to protect against malware (including viruses, worms, spyware, trojans and more) that can infect devices. In addition, with the Application Control feature, it checks whether the applications installed on users' devices are safe and prevents malware from infecting the device.

Advanced Machine Learning: It protects mobile devices against known and emerging threats, blocks access to malicious and phishing websites, and enables secure financial transactions online.

C-Prot Self Defense: The C-Prot EAD SDK Self-Defense feature provides protection by preventing third-party attacks against your application's security layer. Self-defense mechanisms allow you to verify the application's digital signature and detect debugging and injection attempts.

EMBEDDED APPDEFENSE

Application developers can be easily integrated into their existing projects or new application development processes. It is equipped with advanced threat detection and intrusion prevention features. These features proactively protect applications against malicious activity and keep user data secure. It offers a solution for all stakeholders who want to increase mobile application security. It detects keylogger software, blocks malware that records every keystroke of the user and continuously monitors the user. With C-Prot Remote Administrator you can manage your applications from anywhere. This management tool can detect whether the apps on your devices are running in debug mode and determine whether they are running on a rooted/jailbroken device. It helps you determine whether the screen reader is turned on while using the application, whether it is running on a real device, and whether screenshots are taken. It also checks that the running SDK code has not been modified at runtime and that no malicious code has been added. You can also determine whether the certificate used in communication with the server is secure. You can view the list of your devices, the operating system used, IP address, brand and model information. It is a comprehensive solution developed to ensure the security of your mobile applications and provide protection against malware.

Anti-Keylogger Keylogger software that records every keystroke you make and continuously monitors you is detected.	✓
Central Management Console Manage all your endpoints from anywhere with C-Prot Remote Administrator, which can be used as cloud-based or On-prem.	✓
Anti-Debugging It detects that the application is running in debug mode.	✓
Root/Jailbreak Detection It is determined whether the application is running on a Root/Jailbroken device.	✓
Screenshot Control Detects when a screenshot is taken while using the application.	✓
Anti-Injection It is checked that the running SDK code is not changed at runtime and that no malicious code is added.	✓
SSL-Pinning It determines whether the certificate is secure in communication with the server.	✓
Device List You can view the list of your devices, the operating system it uses, the iP information it uses while communicating, the brand and model.	✓
Overlay Detection The Overlay detection feature detects whether users have an overlay on their screen when using an application. Overlay attacks are used to capture users' personal and financial data. It provides a secure user experience by detecting such attacks.	✓
Suspicious Call Detection While using the application, calls from unknown, suspicious numbers or fraud attempts are detected.	✓

C-Prot Cyber Security Kiosk

Designed as a digital security officer that monitors portable media devices.

Top Features

Anti-Malware
It provides multi-layered protection to prevent and neutralise viruses and malware.

Easy-to-Use Web Management Panel
C-Prot Remote Administrator offers you a practical management experience with its easy-to-use management feature.

Full Control with Security Policies
You can monitor the behaviour of removable media devices by defining customisable policies through the management console.

Detailed Report
You can easily view scan reports of removable media devices from the kiosk or management console.

Sectors Used

Critical Infrastructure:
It is placed at critical points of energy companies and infrastructure providers to protect organisations against cyber threats.

Government:
It can be deployed at critical points in governments, defence ministries and public institutions to protect against cyber threats.

Defense Industry:
It scans all kinds of portable devices (USB drives, external discs, smartphones, etc.) of employees working in critical infrastructures such as defense industry and detects potential threats.

Finance:
It is placed at the entrances of banks and financial institutions, allowing them to securely protect their customers' financial information.

Transportation:
It can be used to provide protection against cyber threats by placing it at critical points of organisations operating in the fields of airlines, railways, ports and highways.

Telecommunications:
It provides protection against cyber threats that may come through portable media devices by placing them at critical points of organisations such as telecommunication companies and internet service providers.

CYBER SECURITY KIOSK

C-Prot Cyber Security Kiosk is designed as a digital security guard that inspects devices for malware, vulnerabilities and sensitive data. C-Prot Cyber Security Kiosk is a powerful security solution that supports your company or organisation's digital security strategy. It audits the use of removable media devices, detects security vulnerabilities, and protects your organisation against potential threats by blocking malware.

Automated Threat Removal and Quarantine C-Prot Cyber Security Kiosk automatically cleans or quarantines threats and malicious files detected during scanning.	✓
Central Management Console Manage all your endpoints from anywhere with C-Prot Remote Administrator, which can be used as cloud-based or On-prem.	✓
Supported Media Devices Supports portable media types such as USB, Type-C, CD, DVD, Blu-Ray, Card Reader, SD Card.	✓
Trusted Media Device Only removable media devices that have been pre-determined and verified as secure may be used within the organization. In this way, access of unknown or potentially threatening removable media devices to the corporate network is prevented.	✓
Preferred Solution In various industries such as finance, healthcare, education and government, C-Prot Cyber Security Kiosk is preferred as a reliable solution for securing removable media.	✓
Customize Customizable options are offered regarding the user interface and language options in line with user needs.	✓
Technical Support You can send your 24/7 online support requests to support@c-prot.com support mail address.	✓

C-Prot

www.c-prot.com

www.c-prot.com